6,097,811

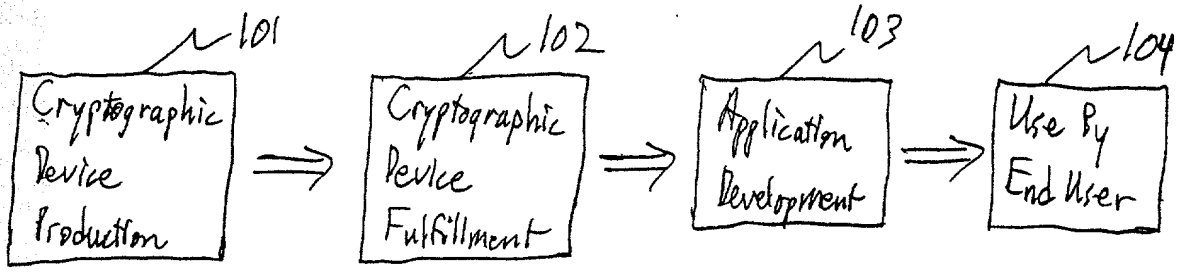

FIG. 1

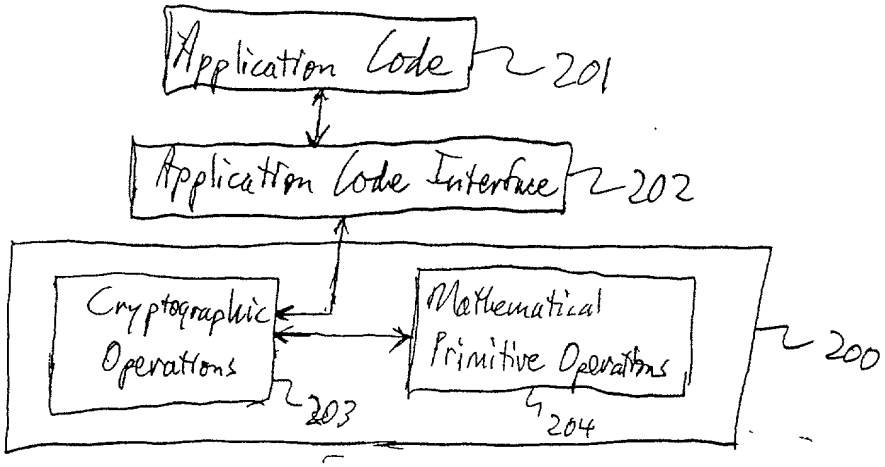

FIG. 2
(Prior Art)

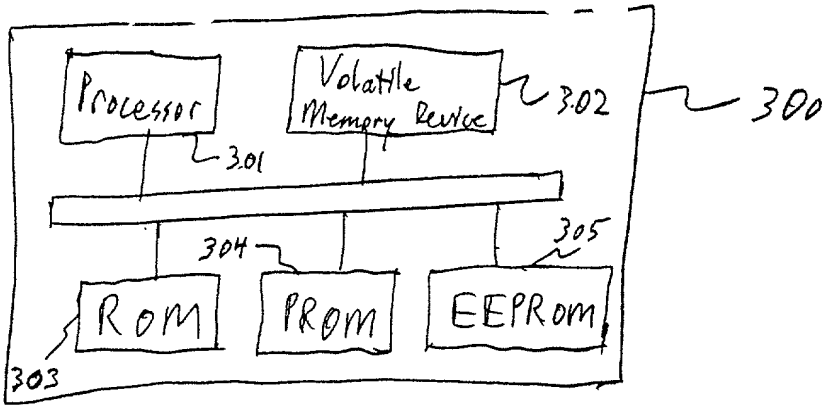
Processor
Volatile Memory Device
302
300
301
304
305
ROM
PROM
EEPROM
303

FIG. 3.

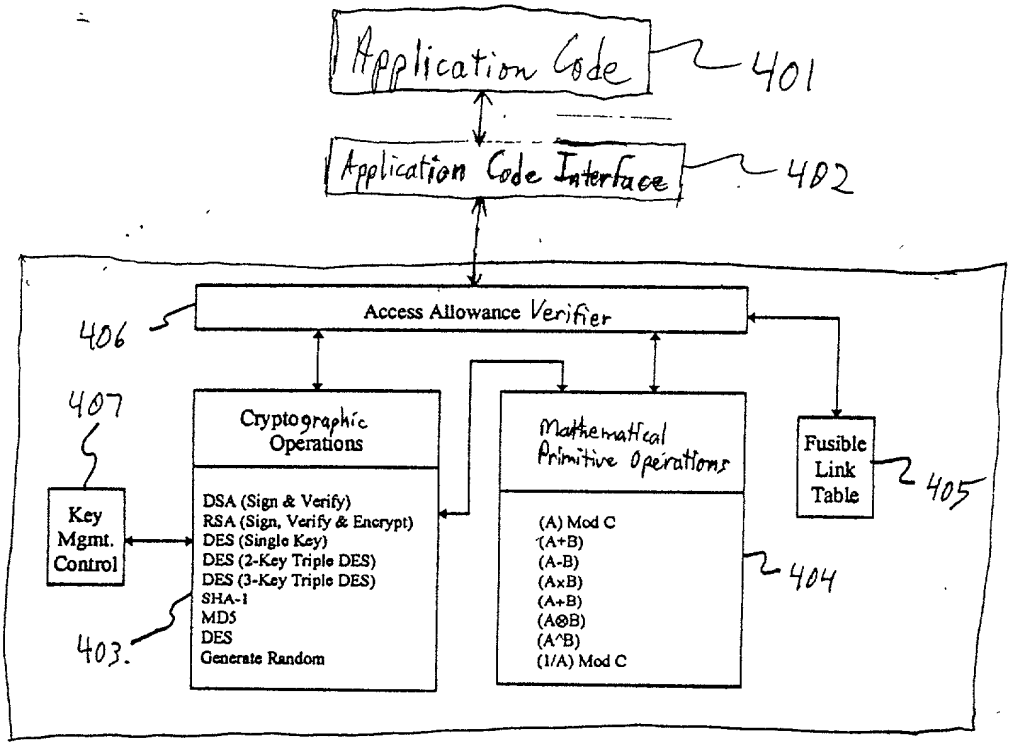
Application Code
401
Application Code Interface
402
Access Allowance Verifier
406
407
Cryptographic Operations
Mathematical Primitive Operations
Fusible Link Table
405
Key Mgmt. Control
DSA (Sign & Verify)
RSA (Sign, Verify & Encrypt)
DES (Single Key)
DES (2-Key Triple DES)
DES (3-Key Triple DES)
SHA-1
MD5
DES
Generate Random
403
(A) Mod C
(A+B)
(A-B)
(AxB)
(A÷B)
(A⊗B)
(A^B)
(1/A) Mod C
404

FIG. 4